Computer Security Technology Center

SSDS - Secure Software Distribution System

by

Tony Bartoletti

Contact: Lauri Dobbs, SSDS Project Leader, LLNL
(925) 423-8590 or e-mail ssds@cheetah.llnl.gov

sponsored by

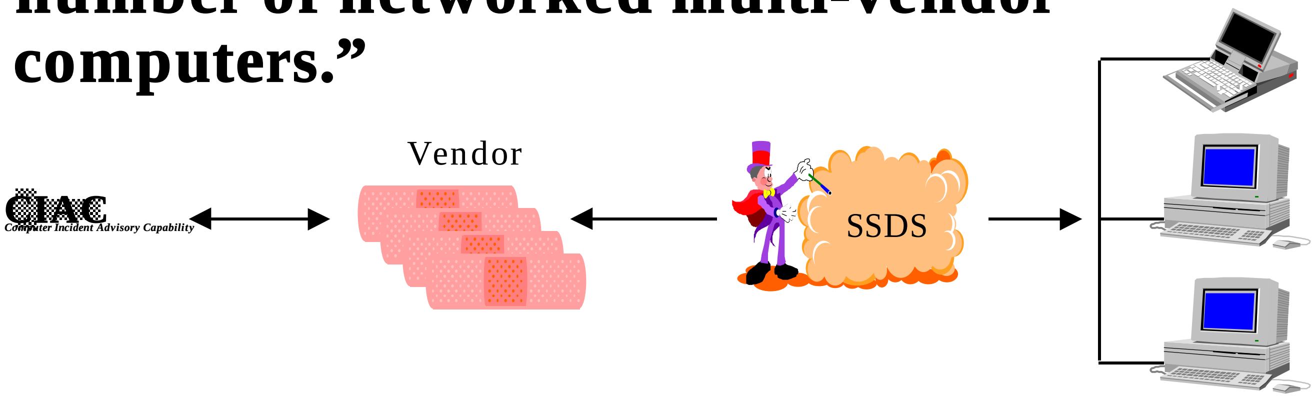
DOE Energy Research

UCRL-MI-127241

This work was performed under the auspices of the U.S. Dept. of Energy at LLNL under contract no. W-7405-Eng-48.

The Goal of SSDS

“To provide an automated means to rapidly evaluate, distribute, and install software security patches in a secure fashion on a large number of networked multi-vendor computers.”



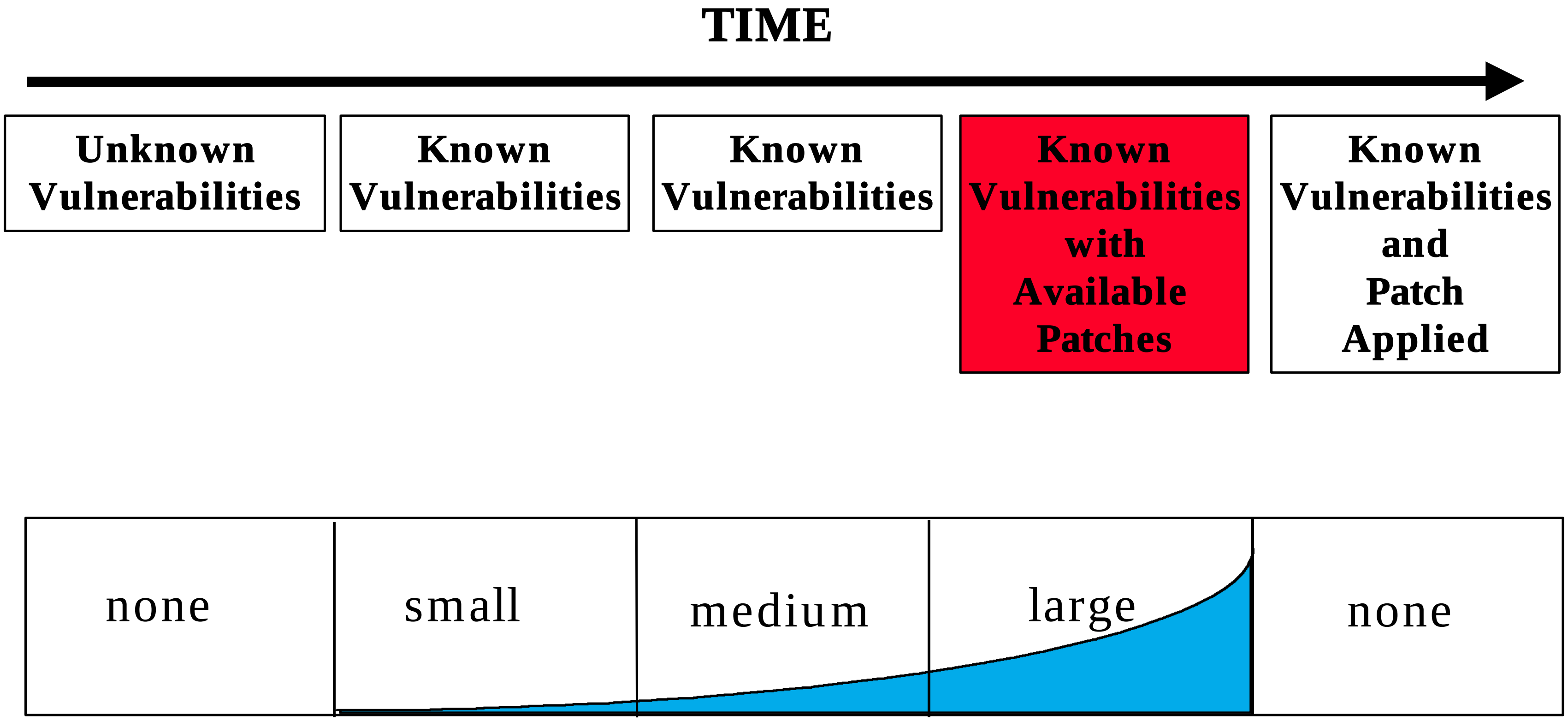
Results:

Greatly enhanced system security and integrity.

SSDS Motivation

- Maintenance of computer systems is a significant portion of the cost of ownership. SSDS reduces this cost by providing transparent system administration.
- Multi-vendor computing environments are the norm, not the exception. SSDS is vendor independent: it will work with any vendor's computing systems.
- System administration is labor intensive and requires specialized knowledge. SSDS leverages the skills and time of system administrators.
- Networked computer systems are vulnerable to viruses, trojan horses, and other malicious software. SSDS provides a comprehensive mechanism to evaluate and validate system's software of networked computers.

Software Vulnerability Timeline



TIME

Unknown Vulnerabilities

Known Vulnerabilities

Known Vulnerabilities

Known Vulnerabilities with Available Patches

Known Vulnerabilities and Patch Applied

none

small

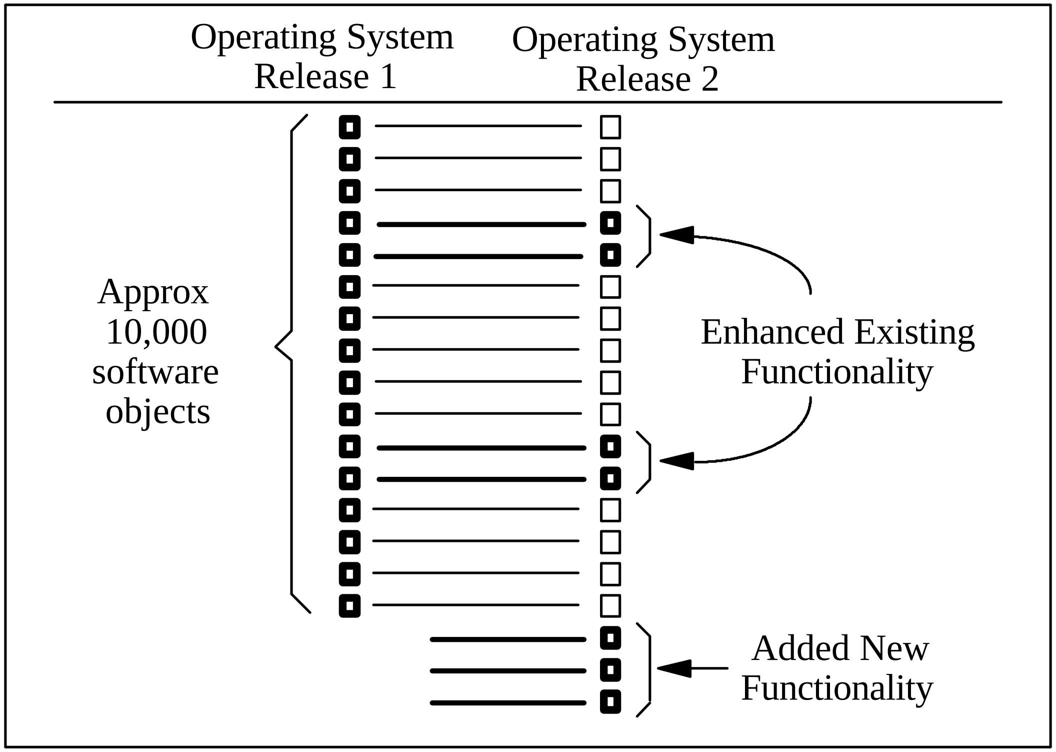
medium

large

none

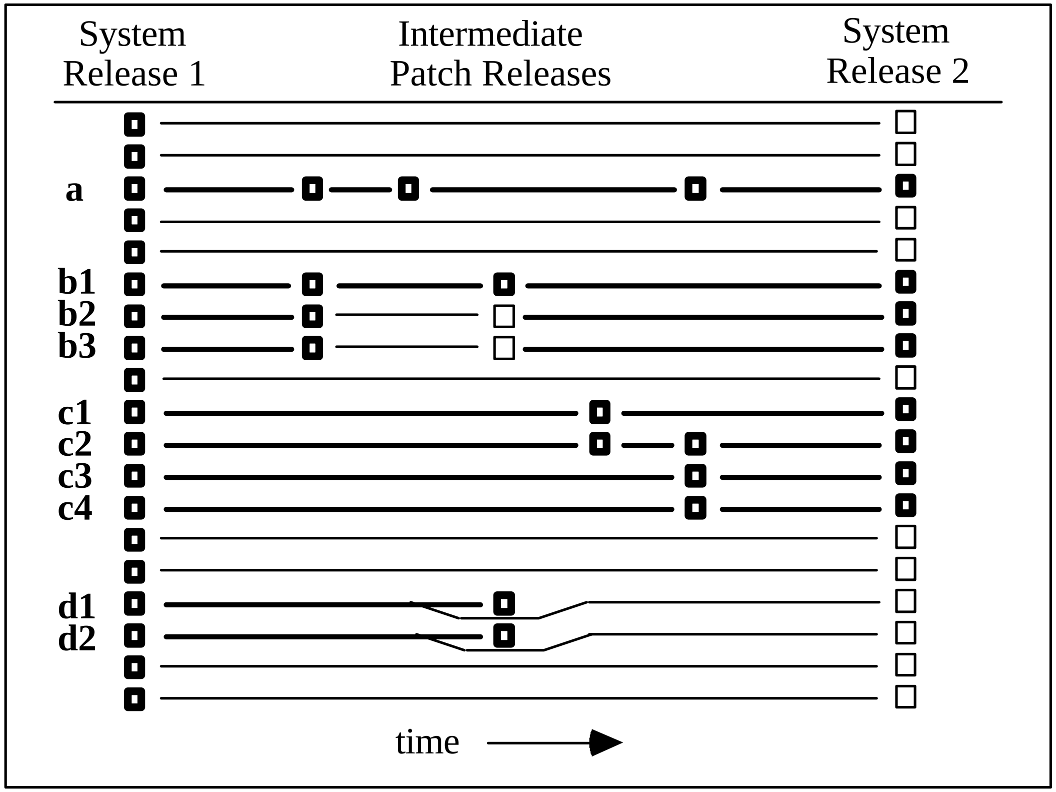
Risk of being exploited

Operating System Upgrade



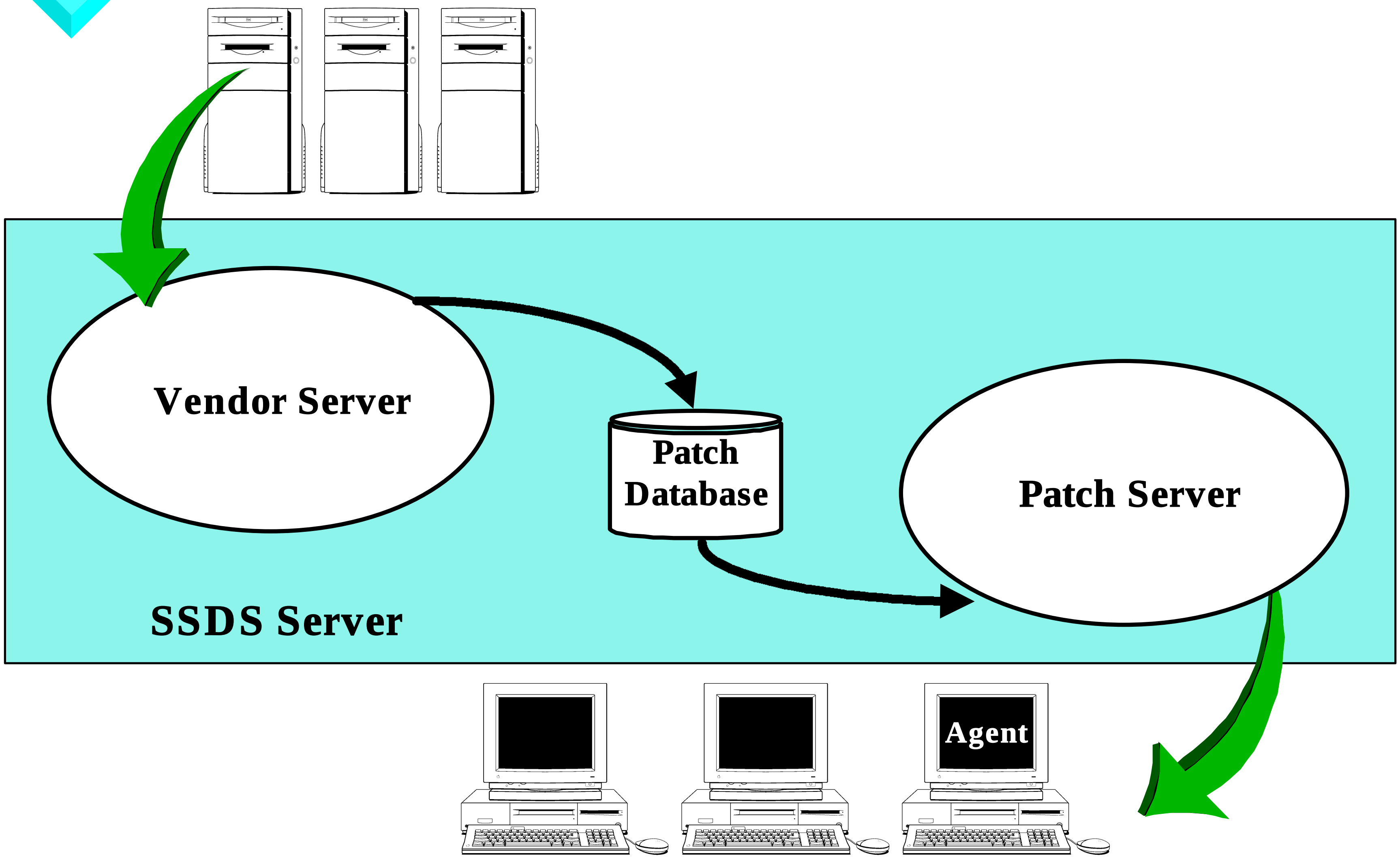
Hundreds of software modules added or modified

Upgrades - The Ugly Reality



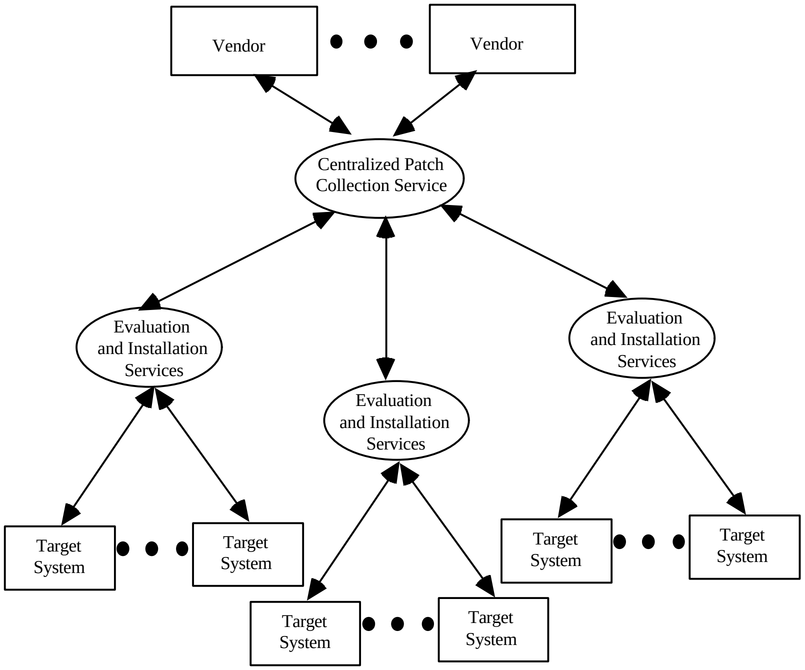
Patch conflicts and contingencies abound

SSDS Architecture



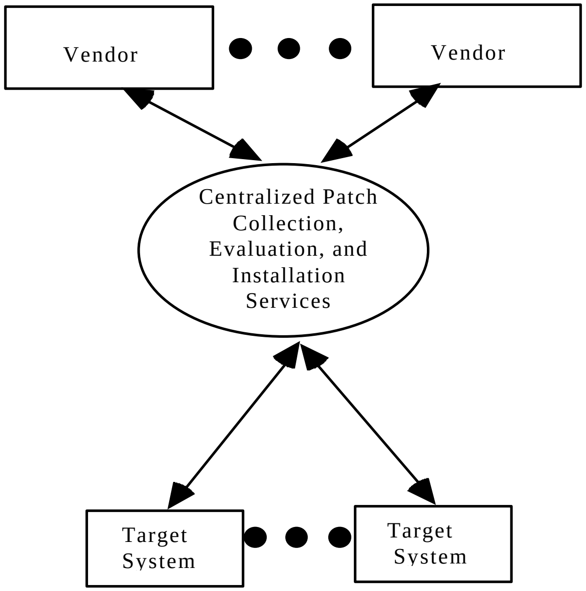
How SSDS Works

- Many networks and hundreds of computers.



Vendor
• • •
Vendor
Centralized Patch Collection Service
Evaluation and Installation Services
Evaluation and Installation Services
Evaluation and Installation Services
Target System
• • •
Target System
Target System
• • •
Target System
Target System
• • •
Target System

- One network and few computers.



Vendor
• • •
Vendor
Centralized Patch Collection, Evaluation, and Installation Services
Target System
• • •
Target System

Where are we today?

- **Completed a proof-of-concept prototype.**
  - **Detect patch deficiencies on Sun systems running Solaris 2.3 and higher.**
  - **Report patches needed to be installed and what is currently installed.**
  - **Monitor and collect Sun patches.**
- **Built a complete history of Sun Solaris patches.**
- **Distributed SSDS prototype to LLNL users for internal review.**

What are we working on now?

- **Broaden range of vendor systems to HP and Digital.**
- **Address secure communications between networked processes.**
- **Distribute needed patches to remote systems.**

Future Goals

- **Automated installation of patches.**
- **Ability to “back out” installed patches.**
- **Broaden range of vendor support to Windows NT.**
- **Broaden range of patch types to include:**
  - **Patches that require editing of configuration files.**
  - **Patches that replace objects in run-time libraries.**
  - **Kernel patches.**

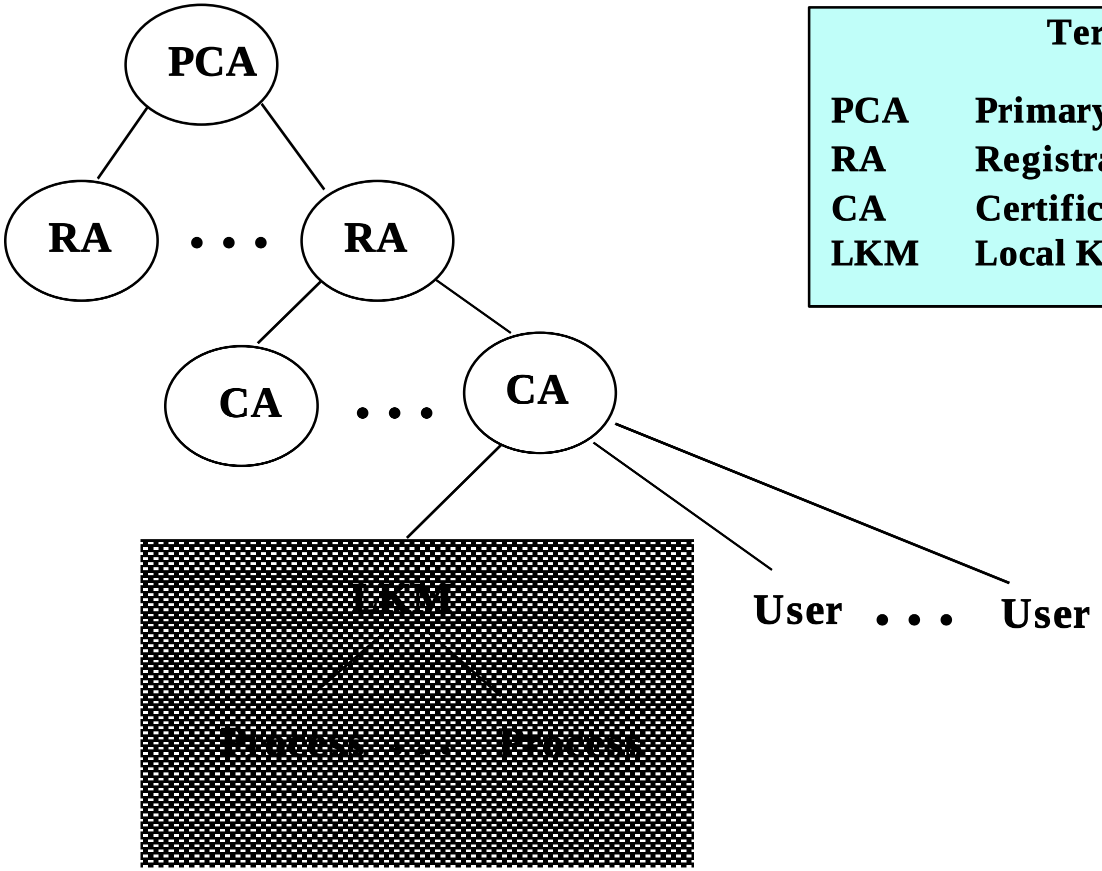
Possible Vulnerabilities

- **SSDS Server**
  - **integrity, authentication and confidentiality**
- **Vendor FTP Servers**
  - **integrity and authentication**
- **Patch Database**
  - **integrity and authentication**

Need Lightweight KI for Distributed Applications

- **Authentication of processes**
  - **SSDS Sever and SSDS Agent**
- **Trust relationship inherent in restricted domains**
  - **Minimal need for cross certification for chaining of CAs**
- **Local, immediate key generator (frequent re-certifications)**
  - **Changing network configuration**
  - **Compromised system**
- **Capability to change CA (LKM)**
  - **New system administration**

Users are “CA”s for Processes



Terms

PCA	**Primary Certification Authority**
RA	**Registration Authority**
CA	**Certification Authority**
LKM	**Local Key Manager**

Conclusion

- **We need** simple **policies and** simple **implementations for** simple **problems.**
- **We need standards for formats and processing.**